# West Virginia

# State Privacy Office

## 2013 Annual Report

A Report by the State Privacy Office

West Virginia Health Care Authority

December 2013

# Executive Branch Departments

- Governor's Office
- Health Care Authority
- Bureau of Senior Services
- Department of Administration
- Department of Commerce
- Department of Education and the Arts
- Department of Environmental Protection
- Department of Health and Human Resources
- Department of Military Affairs and Public Safety
- Department of Revenue
- Department of Transportation
- Department of Veterans Assistance
- Chapter 30 Licensing Boards

# INTRODUCTION

The purpose of this annual report is to depict the Privacy Management Team's (PMT) ongoing activities concerning the advancement of processes undertaken to protect the privacy of personally identifiable information (PII)[1], such as social security numbers, health information, employees' home addresses and driver's license numbers collected and maintained by Executive Branch departments[2]. The report will detail the major accomplishments of the PMT, as well as address new initiatives the PMT is undertaking to further advance its mission and vision.

## Mission

The mission of the PMT is to facilitate West Virginia's vision of implementing best practices and legal requirements to protect PII. The PMT strives to improve data protection and quality and protect the privacy interests of all West Virginians.

## Vision

The PMT recognizes that privacy is a core value of West Virginia citizens and government. The PMT's vision is to ensure:

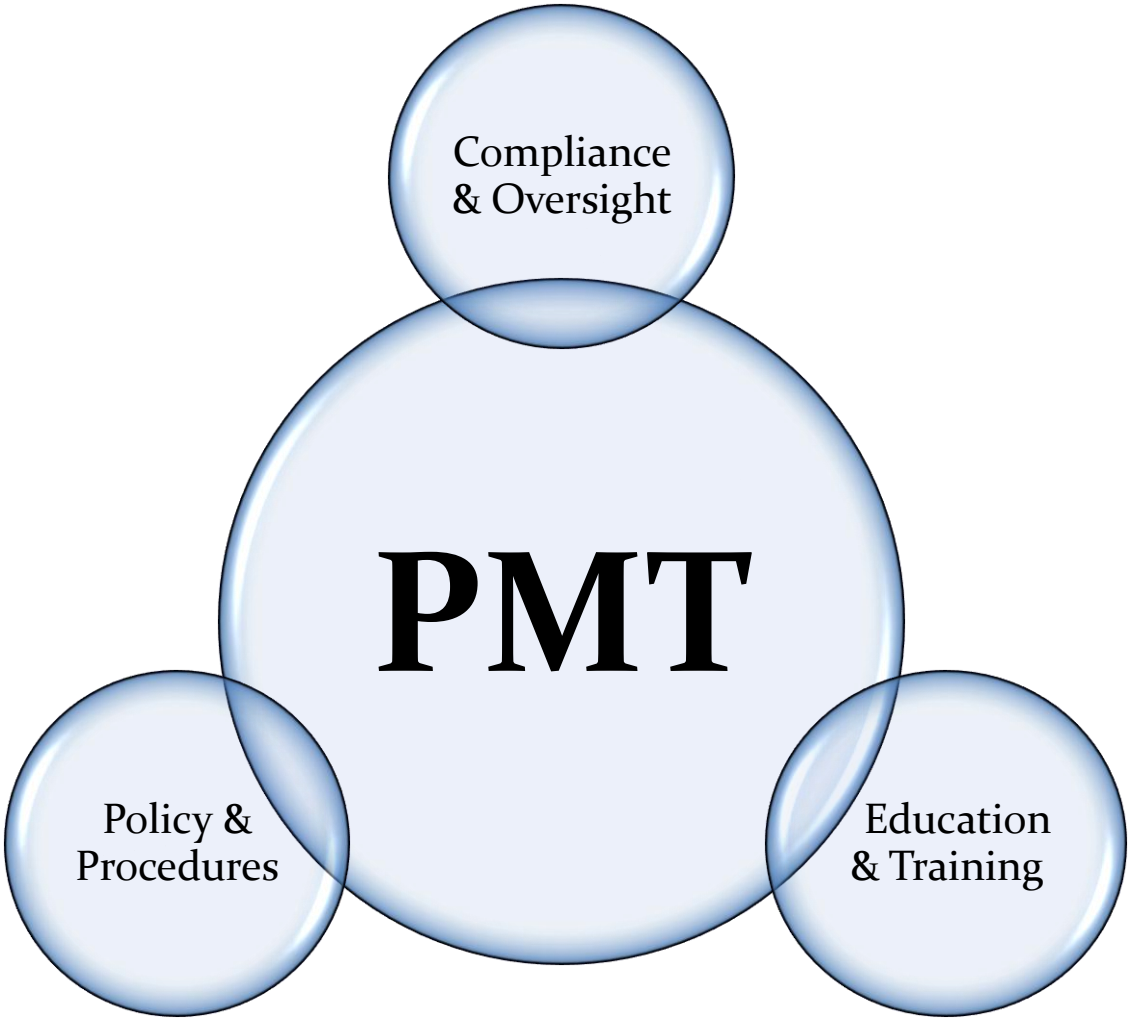
[1]**Personally Identifiable Information (PII):** All information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes Protected Health Information (PHI). PII is contained in public and non-public records. Examples may include but are not limited to a specific individual's: first name (or initial) and last name (current or former); geographical address; electronic address (including an e-mail address); personal cellular phone number; telephone number or fax number dedicated to contacting the individual at his or her physical place of residence; social security account number; credit and debit card numbers; financial records, including checking, savings and other financial account numbers, and loan accounts and payment history; consumer report information; mother's maiden name; biometric identifiers, including but not limited to, fingerprints, palm prints, facial recognition, full face image and iris scans; driver identification number; birth date; birth, adoption or death certificate numbers; physical description; genetic information; medical, disability or employment records, including salary information; computer information, including information collected through an Internet Cookie; and criminal records and history. When connected with one or more of the items of information specified above, PII includes any other information concerning an individual that, if disclosed, identifies or can be used to identify a specific individual physically or electronically.

[2]**Department:** A major division of the Executive Branch of state government that is responsible for administering a specific program area. As used in these policies a department includes its subdivision, bureaus, agencies, boards, commissions, councils, offices and other similarly situated entities.

- Implementation of laws, regulations, best practices, policies and procedures to protect PII;
- Protection of citizens' and employees' PII; and
- Improvement of data quality and protection to enhance West Virginia State Government.

## PMT: 2013 OBJECTIVES

In 2013, the PMT strived to meet its mission and vision by focusing on the following key privacy program objectives:



# COMPLIANCE & OVERSIGHT

To accomplish its mission, the PMT assures that each Department complies with privacy policy and procedures to protect PII. The State Privacy Office (SPO) provides consultation and research to support the PMT and Departments as they integrate measures to ensure improvement of data quality and the protection of citizens' and employees' PII.

## Confidentiality Agreement

Along with privacy training, one of the biggest weapons in the arsenal against insider threats is execution of a strong confidentiality agreement. The West Virginia Executive Branch Confidentiality Agreement sets forth the terms and conditions required of every member of the workforce with respect to confidential data. These terms and conditions are effective throughout the lifetime of the worker. In 2013, Confidentiality Agreement enrollment was completed on the State's Learning Management System (LMS) resulting in at least 67% completion[3] by all Executive Branch departments.

[3] The percentage may not reflect inactive employees or employees who manually take the training.

## Consultation & Research

The SPO provided the Department Privacy Officers (DPO) and Departments the following consultation and research services in 2013:

- Provided privacy legal advice and consultation regarding privacy policies, procedures, laws, regulations, best practices, implementation, and privacy in project design.
- Worked to ensure that there is a Privacy Officer in every department and followed up with the Governor's Office as necessary.
- Made sure that each DPO understood their role and responsibilities, received new privacy officer orientation and training and were given any assistance needed.
- Provided advice and consultation regarding proposed statutory or regulatory changes.
- The SPO's website (www.privacy.wv.gov) was given a fresh, new look and has been updated and reorganized. New graphical designs were added early in 2013.
- The SPO along with PMT members continued to support the wvOASIS project. wvOASIS (Our Advanced Solution with Integrated System) is an Enterprise Resource Planning (ERP) system which comprises a suite of commercially-available integrated modules that allows an organization to use a system of integrated applications to manage its business functions. The purpose of this system will be to centralize transactional data that is useful in tracking, reporting, and providing transparency to State government functions. The Governor, State Auditor, State Treasurer, and Legislature recognize the benefits an ERP system will provide to the State of West Virginia. Representatives from the wvOASIS project attended PMT meetings in 2013 and provided status reports related to the PII identification and requirement process.

## HIPAA/HITECH [4]

- Revised the Notice of Privacy Practices.[5]
- Revised policies/procedures: (1) incident response; (2) the sale of PHI; (3) marketing activities, and review of any relevant contracts; (4) fundraising; (5) requests to restrict disclosure of PHI to health plans from individuals who pay "out of pocket"; (6) requests for access to PHI in electronic format; (7) requests to transmit copies of PHI to third persons; (8) disclosure of the PHI of deceased patients to family members; (9) disclosure of immunization records; and (10) authorizations for research.
- Applied the HIPAA preemption analysis to new policies to ensure application of any more stringent WV law.
- Revised the WV Business Associate Agreement and evaluated agency/vendor relationships.
- Revised authorizations regarding the sale of PHI and marketing.

## Incident Response

In order to ensure adherence with state privacy policy, as well as federal and state privacy laws, the SPO continued to provide incident response support to all Executive Branch DPOs. The SPO served as a resource, offering guidance and advice throughout the incident process, from the initial report, throughout the investigation, until the privacy incident was resolved.

[4] Health Information Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act (HITECH Act).

[5] Notice of Privacy Practices: Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. In January 2013 the Office for Civil Rights (OCR) in the Department of Health and Human Services issued its Omnibus Final Rule, which includes modifications to the HIPAA Privacy and Security Rules under the HITECH Act. Covered entities must update and post a revised Notice of Privacy Practices (NPP) prior to September 23, 2013, compliance deadline.

## Privacy Self-Assessment

In late 2010, a partnership was formed between the West Virginia Health Care Authority (HCA) and the West Virginia Board of Risk and Insurance Management (BRIM). BRIM provides casualty insurance coverage for all state agencies, including protection against lawsuits and other liability claims resulting from incidents. BRIM agreed to support the PMT through financial incentives to agencies within the Executive Branch, as well as agencies outside the Executive Branch to complete privacy self-assessments and this support has continued to date. A privacy self-assessment is a tool designed to help privacy professionals assess their privacy programs. Executive Order No. 6-06 empowers the HCA to conduct audits of privacy programs. The PMT selected the *Generally Accepted Privacy Principles* (GAPP) as the audit framework[6] as it is based upon fair information practices and contains criteria of good privacy practices found in privacy laws and regulations, both nationally and internationally.

The 2013 self-assessment asked departments to certify: a) the number of employees (employed as of May 31, 2013) who have signed confidentiality agreements, b) all privacy policies have been implemented, c) all existing employees on board as of May 31, 2013 had received privacy training, d) all laptops with PII, including PHI, had been encrypted, and e) the self-assessment for the following principles had been completed; Management, Notice, Choice & Consent, Collection, Disclosure to Third Parties, Access, Security for Privacy, Quality and Monitoring & Enforcement. Roll-out for the 2013 privacy self-assessment began July 1 with a completion date of November 18, 2013 for the survey. The self-assessments were completed by DPOs and Agency Privacy Officers, then reviewed and certified by their respective Cabinet Secretaries.

[6] The audit framework (GAPP) is designed to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities. The primary objective is to facilitate privacy compliance and effective privacy management. The secondary objective is to provide suitable criteria against which a privacy attestation engagement (usually referred to as a privacy audit) can be performed.

The self-assessments and certifications were submitted to the SPO by November 22, 2013, with a completion rate of 99% by Executive Branch agencies, excluding the Chapter 30 Licensing Boards.

# EDUCATION & TRAINING


## Data Privacy Day

For the third consecutive year, the West Virginia Executive Branch championed *Data Privacy Day*, January 28, 2013 as a day to highlight the importance of the protection of personal and private data, and remind us to remain vigilant and proactive about protecting the information that others have entrusted to us. The genesis of *Data Privacy Day*, in the United States and Canada, was in January 2008 and was an extension of the *Data Protection Day* celebration in Europe. The United States Senate issued a resolution, sponsored by Senator John D. Rockefeller IV, recognizing January 28th as *National Data Privacy Day* for the fourth year in a row.

In furtherance of the support of *Data Privacy Day*, Governor Earl Ray Tomblin issued a Proclamation declaring January 28, 2013 as *Data Privacy Day* in West Virginia. The Proclamation recognized Executive Order No. 6-06, giving the Chair of the HCA the

responsibility for protecting the privacy of PII collected and maintained by Executive Branch agencies. The HCA leads and staffs the team and houses the SPO for the Executive Branch. The Governor's Proclamation is a yearly reminder that we all share the responsibility to be conscientious stewards of data by respecting privacy, safeguarding data and enabling trust. *Data Privacy Day* is an effort to empower and educate people to protect their privacy, control their digital footprint, and make the protection of privacy and data a great priority in their lives.

Additional *Data Privacy Day* activities included a *Privacy After Hours* event. The International Association of Privacy Professionals (IAPP) approved the SPO to host a *Privacy After Hours* event held on January 23, 2013. *Privacy After Hours* provided a wonderful opportunity to meet other privacy professionals from the area, network, and engage in lively discussion in a relaxing environment.

## PMT Professional Development

The HCA chairman and Executive Director approved sponsorship for the 2013 Privacy Retreat held October 15-17, 2013 at Stonewall Resort. The primary goal of the 2013 Privacy Retreat was to: 1) provide WV Executive Branch PMT members an opportunity to enhance their skills in the area of privacy, security and incident response; and 2) bring the PMT members together and allow them to learn from one another, share their knowledge, views and experiences for everyone's benefit. This year's speakers represented the private sector as well as federal and state government who presented and discussed the latest topics in cyber security, BYOD (bring your own device), privacy engineering as well as focusing on strategies, experiences and techniques with regard to the incident process including pro-active measures. Margaret (Peggy) Eisenhauer, J.D., CIPP/US, founder of Privacy & Information Management Services, was the primary facilitator for this event. A total of 25 attendees participated in this event. On October

18, 2013 all attendees (including speakers) were invited to complete an online evaluation form. Twenty-two out of the 25 invitees completed the evaluation – a response rate of 88%. The overall privacy retreat experience was rated 4.58 on a five-point scale, which is between "very good" and "excellent." Ratings for each speaker and/or session were in the same range.

## Workforce Development

The SPO and PMT embarked on a project to develop a three-year (2012-2015) training plan to ensure that employees receive appropriate training and education regarding privacy laws, regulations, policies, standards, and procedures governing the handling of PII. In 2013, the following trainings were provided:

### Privacy Awareness

- *Privacy Rocks!* This training is offered through the WV State Learning Management System (LMS). The training provides an overview of what is privacy, how to handle personal information, privacy responsibility and privacy policies.
- Who is required to take this training? All Executive Branch Workforce
- In 2013, *Privacy Rocks!* enrollment was completed, resulting in 69% completion by all Executive Branch departments. (Percentage may not reflect inactive employees and/or employees that manually take the training .)

### HIPAA/HITECH

- On February 17, 2009, the HITECH Act was signed. The HITECH Act is part of the American Recovery and Reinvestment Act of 2009 or ARRA. Four years later, regulations known as the Final Omnibus Rule were promulgated with an effective date of March 26, 2013. Compliance for Covered Entities and Business Associates was required by September 23, 2013.
- To assist Executive Branch Covered Entities and Business Associates with compliance by September 23, 2013, the SPO provided six one-day training sessions from June to August 2013. The training was required for DPOs from Departments with a HIPAA impact.

## WV Executive Branch Privacy Awareness Training Wins International Award

In the fall of 2012, the SPO developed a new privacy awareness training entitled "*Privacy Rocks!*" with the help of MediaPro. This course is required for all Executive Branch employees. It covers privacy basics, including helping employees understand their responsibilities with respect to privacy, the importance of privacy, how to safeguard personal information and how to report an incident. Privacy touches the entire life cycle of information management, from data collection and vendor management to records management, information and technology security and records destruction. The training is delivered through the Office of Technology's (OT) LMS which allows all employees with a computer to be able to complete the training at their own desks, and when it fits into their schedule. For employees without access to computers, completion of the training course is confirmed in the LMS system as well. *Privacy Rocks!* won the bronze award in the "Training/E-learning" category from Horizon Interactive Awards. Horizon Interactive Awards is a prestigious international competition that recognizes outstanding achievement for interactive media producers. Entries are judged on solution creativity and originality, overall graphic design, appearance, user experience, communication of message, technical merit, and the effectiveness of solution.

# POLICY & PROCEDURES


## Privacy Requirements

Each Department must operate within its legal authority and restrictions with regard to the collection, use, disclosure and retention of PII. The Privacy Requirements document reviews laws that impact the enterprise. Necessarily, there will be privacy laws not covered in the report, as they impact isolated agencies. This report is updated on an annual basis, with issuance in the fall of each year. Laws are divided into two categories, Federal and State. Each law is identified by its common name, legal citation with a description, implications and electronic source.
The 2013 update to the West Virginia Executive Branch Privacy Requirements includes all relevant privacy legislative and congressional enactments, regulations, and court decisions since June 2012. This online resource is used by privacy professionals and communicated to the West Virginia State Bar.

## Revised Response to Unauthorized Disclosures Procedure

The *Response to Unauthorized Disclosures* procedure was revised and finalized for distribution in August 2013. This procedure was revised to bring it into compliance with the HITECH Act, which had a compliance deadline of September 23, 2013. This procedure applies to all

Departments (including the Governor's Office, agencies, boards and commissions) within the Executive Branch of the West Virginia State Government, excluding other constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, County Boards of Education, and the Public Service Commission.

# LOOKING AHEAD IN 2014

## Compliance & Oversight

- **Privacy Impact Assessment (PIA):** PIA is a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed implementation of a system. PIAs are considered a key component of privacy programs. All organizations need to implement processes to identify projects that impact privacy and build in key controls during the earliest stages of those initiatives. The approach to PIAs may vary and may need to be adapted or specific to the organization. In 2014, the SPO will research best practices for ensuring that the WV Executive Branch has PIA processes in place.
- **BYOD (Bring Your Own Device):** BYOD programs allow employees to use their own devices (smart phones, tablets, laptop, & computers) to access data from or complete work related tasks for their employers. Research shows that while BYOD programs

result in increased employee productively and job satisfaction, they also bring privacy and security challenges. In 2014, the SPO will be working with OT to outline best practices for the WV Executive Branch BYOD program.

- **Consultation & Research**: The SPO will continue to provide DPOs and Departments with on-going support with their privacy questions and privacy related consultation and research.
- **Privacy Self-Assessment:** In an ongoing commitment to protect privacy and reduce liability, the HCA and BRIM will continue to partner by convening a workgroup to evaluate the 2013 privacy self-assessment and shape the 2014 assessment. In 2014, the following principle(s) will be added to the assessment: Use, Retention and Disposal.
- **wvOASIS:** The SPO will continue to coordinate with wvOASIS to facilitate privacy implementation for the project and will provide advice and consultation as requested. Additionally, the SPO will serve as a liaison between the wvOASIS project team and the DPOs to ensure privacy objectives are met in a way that is beneficial to the project.

## Education & Training

- As an ongoing demonstration of support for privacy efforts in West Virginia, the SPO will be asking Governor Earl Ray Tomblin to issue a Proclamation declaring January 28, 2014 as Data Privacy Day in West Virginia. Data Privacy Day 2014 will focus on the following; "Respecting Privacy, Safeguard Data and Enabling Trust." To celebrate this day, the SPO will orchestrate a variety of privacy awareness events and activities for the West Virginia workforce, to highlight the importance of protecting personally identifiable information. Combined activities will also include providing privacy awareness tips and a *Privacy After Hours* networking event.

- The SPO will continue to support each DPO with their overall privacy training program which will include privacy awareness training for new work force members, on-going professional development of DPOs and privacy awareness tips.

## Policy & Procedures

- The SPO and PMT will review the West Virginia Executive Branch Privacy Requirements for any relevant updates based upon privacy legislative and congressional enactments, regulations, and court decisions.

# CONCLUSION

Management of privacy risks is a key objective of the overall PMT program. In 2013, Department level self-assessments of their privacy program remained steady for ensuring their privacy compliance obligation. In 2013, the Executive Branch DPOs and agency level Privacy Coordinators focused on ensuring privacy awareness training and compliance within the West Virginia workforce. Again in 2013, it was a great honor to have Governor Earl Ray Tomblin sign a Proclamation designating January 28 as *Data Privacy Day* in West Virginia. The SPO provided additional support by providing professional development opportunities for DPO which included HIPAA/HITECH training and the Privacy Retreat. From the numerous requests for additional training, the feedback on privacy tips, and the participation in privacy-related events, it is obvious that privacy is advancing as a priority in the planning and design phases of major projects in state government.

With a robust commitment by the SPO and PMT to prioritize privacy and data protection practices in 2014, citizen trust will be increased and credibility will be elevated. It is anticipated

that 2014 will be a year replete with exciting privacy educational opportunities and an ongoing commitment to protecting the PII entrusted to the Executive Branch of West Virginia state government.